Available online at www.sciencedirect.com

SCIENCE DIRECT®

Theoretical Computer Science 359 (2006) 449–454

Theoretical Computer Science

www.elsevier.com/locate/tcs

Note

Completing codes and the Rédei property of groups

Sándor Szabó*

Institute of Mathematics and Informatics, University of Pécs, Ifjúság u. 6, H-7624 Pécs, Hungary

Received 14 February 2005; received in revised form 5 July 2005; accepted 3 February 2006

Communicated by D. Perrin

Abstract

The Hajós property of groups is extensively used in connection with variable length codes. We will show that a weaker property, the Rédei property, can also be employed for studying completion of codes.

Keywords: Variable length codes; Completing codes; Factoring groups

1. Introduction

If A is a nonempty finite alphabet, then A^* stands for the set of all the possible finite words can be formed using letters from A. With the operation of the concatenation of words A^* is a free semigroup generated by the elements of A. The neutral element is the empty word. A nonempty subset C of A^* is called a *code* if for each $c_1, \ldots, c_u, d_1, \ldots, d_v \in C$ from

$$c_1 \cdots c_u = d_1 \cdots d_v$$

it follows that $u = v$, that is, $c_1 \cdots c_u = d_1 \cdots d_u$. Then it follows that $c_1 = d_1, \ldots, c_u = d_u$. We say that a code C over the alphabet A is *maximal* if for each code C' over A from $C \subset C'$ it follows that $C = C'$. Every code C over A is contained by a maximal code C' over A. A code C is called *complete* if each word of A^* is a factor of some word in C^*. Any complete code C' containing C is called a *completion* of C. If both C and one of its completion C' are finite, then C is *finitely completable*. We have to stress that the notion of maximal and of complete code are in general not equivalent. However, for finite codes it is true that a code is maximal if and only if it is complete. For further details see [1].

Let G be a finite abelian group written additively with neutral element 0. For two subsets A and B of G we define $A + B$ to be

$$\{a + b : a \in A, b \in B\}.$$

* Tel.: +36 72 225633.
E-mail address: sszabo7@hotmail.com.

0304-3975/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2006.02.002

If each element g of G can be represented uniquely in the form

$$g = a + b, \quad a \in A, \ \ b \in B,$$

then the sum $A + B$ is equal to G and we call $G = A + B$ a *factorization* of G. Factoring a finite abelian group into a direct sum of its subgroups is a well-known construction. Here, we do not assume that the factors are subgroups. In 1989, Restivo et al. [5] have found a remarkable necessary condition for a code being finitely completable in terms of factorization of finite cyclic groups. Let Z_n be denote the cyclic group of order n. We always think of Z_n as the set of elements $0, 1, \ldots, n-1$ with the operation of addition modulo n.

Theorem 1. *Let C be a finite code over the binary alphabet $\{a, b\}$ such that $b \in C$. Define the sets*

$$R = \{r : a^r b^i \in C, i \geqslant 1\},$$
$$S = \{s : b^i a^s \in C, i \geqslant 1\}.$$

If C' is a finite completion of C, then there is a positive integer n such that $a^n \in C'$. Further there are $A, B \subset Z_n$ with $R \subset A$, $S \subset B$ and $Z_n = A + B$ is a factorization.

By means of Theorem 1 it is possible to exhibit finite codes which cannot be embedded into a finite maximal code. In fact, many of the known noncompletable codes are constructed in this way. As an illustration we quote a result from [5].

Theorem 2. *Let*

$$C = \{a^n\} \cup \{a^r b, ba^s : r \in R, s \in S\}$$

be a finite code with $b \in C$. If n is a prime and $|R| \geqslant 2$, $|S| \geqslant 2$, then C cannot have a finite completion.

Assume the contrary that C has a finite completion C'. Since $a^n \in C$ it follows that $a^n \in C'$. By Theorem 1, there are $A, B \subset Z_n$ such that $R \subset A$, $S \subset B$ and $Z_n = A + B$ is a factorization. From the factorization we get the factorization $n = |Z_n| = |R||S|$ in integers which is obviously impossible.

Restivo et al. have advanced the following intriguing conjecture.

Conjecture 1. *Let k, n, p be positive integers such that $p, k < n$, p is a prime, $p \not| k$. Let A, B be subsets of Z_n, where $0, 1 \in A$ and $0, p, k \in B$. Then $Z_n = A + B$ cannot be a factorization.*

The results of this note are connected to Theorem 2 and Conjecture 1 and we will use techniques from the factorization theory of abelian groups.

A subset A of a finite abelian group G is defined to be *periodic* if there is an element g of G such that $A + g = A$ and $g \neq 0$. We say that a finite abelian group G has the *Hajós property* if from each factorization $G = A + B$ it follows that at least one of the factors A or B is periodic. We would like to point out that in some papers the groups with Hajós property are termed "good" groups. In a series of papers of C. De Felice the Hajós property has featured prominently. (For example [2,3]. See also [4].) The complete list of finite cyclic groups with the Hajós property is available in [6]. Namely, Z_n possesses the Hajós property if and only if n is a positive divisor of the following numbers:

$$p_1^{\alpha(1)} p_2, \ \ p_1^2 p_2^2, \ \ p_1^2 p_2 p_3, \ \ p_1 \cdots p_4. \tag{1}$$

Here, $p_1, \ldots, p_4$ are distinct primes and $\alpha(1)$ is a positive integer.

For a subset A of a finite abelian group G, $\langle A \rangle$ denotes the smallest subgroup of G that contains A. In other words, $\langle A \rangle$ designates the *span* of A in G. The subset A of G is called *normalized* if $0 \in A$. The factorization $G = A + B$ is termed normalized if A and B are normalized. We say that a finite abelian group G has the *Rédei property* if whenever $G = A + B$ is a normalized factorization of G, then either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. Phrasing it differently either A or B is contained in a maximal subgroup of G. In this note we will present the complete list of finite cyclic groups with the Rédei property. Then we will use these factorization results to gain insight into completing codes.

2. The Rédei property

Let the finite abelian group G be a direct sum of its subgroups H and K. Then each element g of G can be represented uniquely in the form

$$g = h + k, \quad h \in H, \ k \in K.$$

The element h will be called the *H-component* of g and we will denote it by $g_{|H}$. Similarly, we will call k the *K-component* of g and we will use the $g_{|K}$ notation for k. If G is a direct sum of its subgroups H and K such that $|H|$ is a power of the prime p and $|K|$ is relatively prime to p, then H is called the p-component of G. If H is a subgroup of G and there is a subgroup K such that G is the direct sum of H and K, then we say that K is a *complementary direct summand* of H. If A is a subset of G, then $|A|$ stands for the number of elements of A. If a is an element of G, then $|a|$ denotes the order of a.

One can verify easily that if H is a subgroup of G, A, B are subsets of G such that $A \subset H$, then $(A + B) \cap H = A + (B \cap H)$. We will refer to this observation that we restricted the sum $A + B$ to the subgroup H.

Theorem 3. *Let p, q be distinct primes. Let G be a finite abelian group whose p-component and q-component are cyclic. If $G = A + B$ is a factorization of G and $|A| = p^\alpha q^\beta$, then either $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$.*

Proof. Assume that there is a counterexample, that is, there is a factorization $G = A + B$ such that $|A| = p^\alpha q^\beta$ and $\langle A\rangle = \langle B\rangle = G$. Let H be the p-component of G with $|H| = p^\gamma$. Let K be the q-component of G with $|K| = q^\delta$. Set $M = H + K$.

We claim that in a counterexample $G = A+B$ we can replace A by A' such that there is an $a \in A'$ with $|a_{|M}| = p^\gamma q^\delta$.

To prove the claim we can argue in the following way. If $a_{|M} \in pH + K$ for each $a \in A$, then $\langle A\rangle \neq G$. This is not the case. It follows that there is an $a_1 \in A$ such that $a_{1|M} \notin pH + K$. This means $|a_{1|M}| = p^\gamma q^\mu$. If $\mu = \delta$, then we are done. We assume that $\mu < \delta$. If $a_{|M} \in H + qK$ for each $a \in A$, then $\langle A\rangle \neq G$. It follows that there is an $a_2 \in A$ such that $a_{2|M} \notin H + qK$. This means that $|a_{2|M}| = p^\nu q^\delta$. If $\nu = \gamma$, then we are done. We assume that $\nu < \gamma$.

Adding $-a_2$ to the factorization $G = A + B$ we get the factorization

$$G = G - a_2 = (A - a_2) + B = A' + B.$$

Set $a = a_1 - a_2$. Plainly, $a \in A'$. Let $|a_{|M}| = p^e q^f$. From $a + a_2 = a_1$ we get $a_{|H} + a_{2|H} = a_{1|H}$. If $e < \gamma$, then the order of $a_{|H} + a_{2|H}$ is less than p^γ and the order of $a_{1|H}$ is p^γ. This is an outright contradiction. Therefore $e = \gamma$. From $a_2 = a_1 - a$ we get $a_{2|K} = a_{1|K} - a_{|K}$. If $f < \delta$, then the order of $a_{1|K} - a_{|K}$ is less than q^δ and the order of $a_{2|K}$ is q^δ. This contradiction shows that $f = \delta$. Thus, $|a_{|M}| = p^\gamma q^\delta$ and $a \in A'$ as we claimed.

Next, we claim that in a counterexample $G = A' + B$ we may replace B by B' such that there is a $b \in B'$ with $|b_{|M}| = p^\gamma q^\delta$. This claim can be verified in the same way we have just seen.

Let us suppose that $G = A + B$ is a counterexample such that there are $a \in A$, $b \in B$ with $|a_{|M}| = |b_{|M}| = p^\gamma q^\delta$. Let N be the complementary direct summand of M in G and let $|N| = n$. By Proposition 3 of [8], in the factorization $G = A + B$ the factor A can be replaced by nA to get the factorization $G = nA + B = A' + B$. Clearly, N is a complete set of coset representatives of G modulo M. The sets $B \cap (M + c)$, $c \in N$ form a partition of B. There is a $c \in N$ such that $b \in B \cap (M + c)$.

Adding $-c$ to the factorization $G = A' + B$ we get the factorization

$$G = G - c = A' + (B - c).$$

Note that $M = \langle A'\rangle$. Restricting the factorization $G = A' + (B - c)$ to M we get the factorization

$$M = G \cap M = A' + [(B - c) \cap M].$$

Obviously, M is a cyclic group of order $p^\gamma q^\delta$. In the factorization

$$M = A' + [(B - c) \cap M] = A' + B',$$

where $\langle A'\rangle = M$. From $b \in B \cap (M + c)$ we get $b - c \in (B - c) \cap M = B'$. Then $|b_{|M}| = p^\gamma q^\delta$ and $(b - c)_{|M} = b_{|M} - c_{|M} = b_{|M}$ show that $\langle B'\rangle = M$. Now $\langle A'\rangle = \langle B'\rangle = M$ contradict to Theorem 4 of [7].

Table 1

$\lvert Z_n\rvert = n$	$\lvert H_1\rvert$	$\lvert H_2\rvert$	$\lvert H_3\rvert$
$p_1^{\alpha(1)} p_2^{\alpha(2)} p_3^{\alpha(3)}$	$p_1^{\alpha(1)}$	$p_2^{\alpha(2)}$	$p_3^{\alpha(3)}$
$p_1^{\alpha(1)} p_2^{\alpha(2)} p_3 p_4$	$p_1^{\alpha(1)}$	$p_2^{\alpha(2)}$	$p_3 p_4$
$p_1^{\alpha(1)} p_2 \cdots p_5$	$p_1^{\alpha(1)}$	$p_2 p_3$	$p_4 p_5$
$p_1 \cdots p_6$	$p_1 p_2$	$p_3 p_4$	$p_5 p_6$

This completes the proof. □

Theorem 4. *The cyclic group Z_n has the Rédei property if and only if n is a positive divisor of the following numbers*:

$$p_1^{\alpha(1)} p_2^{\alpha(2)} p_3,\ p_1^{\alpha(1)} p_2 p_3 p_4,\ p_1 \cdots p_5. \tag{2}$$

Here, $p_1, \ldots, p_5$ are distinct primes and $\alpha(1)$, $\alpha(2)$ are positive integers.

Proof. Let the finite abelian group G be a direct sum of its subgroups H_1, H_2, H_3, where $|H_1|$, $|H_2|$, $|H_3|$ are composite numbers. A construction in [10] shows that G does not have the Rédei property. Thus, Z_n does not have the Rédei property if n is one of the following:

$$p_1^{\alpha(1)} p_2^{\alpha(2)} p_3^{\alpha(3)},\ p_1^{\alpha(1)} p_2^{\alpha(2)} p_3 p_4,\ p_1^{\alpha(1)} p_2 \cdots p_5,\ p_1 \cdots p_6. \tag{3}$$

Here, $p_1, \ldots, p_6$ are distinct primes and $\alpha(i)$ is an integer at least 2. The details are listed in Table 1.

By Lemma 1 of [11], Z_n does not have the Rédei property if n is divisible by a number from the list (3).

On the other hand, if n is on the list (2) or a positive divisor of a number on this list, then in the factorization $Z_n = A + B$ at least one of $|A|$, $|B|$ has at most two distinct prime divisors. Therefore, Theorem 3 is applicable and gives that $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$.

This completes the proof. □

3. Applications

The first result is a variant of Theorem 2. It facilitates to construct finite codes over a binary alphabet without the possibility of a finite completion.

Theorem 5. *Let n be a positive divisor of one of the numbers on the list* (2). *Let*

$$C = \{a^n\} \cup \{a^r b, ba^s : r \in R, s \in S\}$$

be a finite code. If $0 \in R \cap S$, R contains two relatively prime integers and similarly S contains two relatively prime integers, then C has no finite completion.

Proof. Suppose C has a finite completion C'. Note that $a^n \in C'$ and $b \in C$ as $0 \in R \cap S$. By Theorem 1, there are $A, B \subset Z_n$ for which $R \subset A$, $S \subset B$ and $Z_n = A + B$ is a factorization. Let $u, v \in R$ such that $0 \leqslant u, v \leqslant n-1$ and u, v are relatively prime. There are integers x, y for which $ux + vy = 1$. Then $ux + vy \equiv 1 \pmod n$. This means $\langle A\rangle = Z_n$. Similarly, $\langle B\rangle = Z_n$. On the other hand by Theorem 4, Z_n possesses the Rédei property and consequently either $\langle A\rangle \neq Z_n$ or $\langle B\rangle \neq Z_n$.

This contradiction completes the proof. □

The next theorem is motivated by Conjecture 1.

Table 2

b	a^3b	a^8b	$a^{11}b$
ba	a^3ba^2	a^8ba^2	$a^{11}ba$
ba^7	a^3ba^4	a^8ba^4	$a^{11}ba^2$
ba^{13}	a^3ba^6	a^8ba^6	
ba^{14}			

Theorem 6. *Let k, n, p be positive integers such that $p, k < n, p$ is a prime, $p \nmid k$. Let A, B subsets of Z_n with $0, 1 \in A$, $0, p, k \in B$. If $Z_n = A + B$ is a factorization, then there are primes $p_1, \ldots, p_6$ such that p_1, p_2, p_3 are distinct, p_4, p_5, p_6 are distinct and $(p_1 \cdots p_6) \mid n$.*

Note that in a counterexample to Conjecture 1, n must be at least $(2 \cdot 3 \cdot 5)^2 = 900$. This lower bound was 42 in [5] and 72 in [1] in the special case $p = 2, k = 5$. The lower bound 42 has been found by a computer search. The lower bound 72 is a consequence of the Hajós property. The point here is that one gets a better result with the Rédei property.

Proof. Consider the factorization $Z_n = A + B$. The assumptions of the theorem give that $\langle A \rangle = \langle B \rangle = Z_n$. By Theorem 3, both $|A|$ and $|B|$ must have at least three distinct prime divisors.

This completes the proof. □

In 1985, to refute the triangle conjecture P. W. Shor [9] constructed the code listed in Table 2.

It is undecided if Shor's code has a finite completion. Suppose that Shor's code has a finite completion, say C'. It is known that there is positive integer n such that $a^n \in C'$. In [5] it was shown that $n > 90$ and in [1] it was proved that $330 \mid n$. We improve these results.

Theorem 7. *Suppose that C' is a finite completion of Shor's code and $a^n \in C'$. Then there are distinct primes p_1, p_2, p_3 such that $(330 p_1 p_2 p_3) \mid n$.*

Note that in particular $n \geqslant 9900$.

Proof. The sets R and S associated with Shor's code are

$$R = \{0, 3, 8, 11\}, \quad S = \{0, 1, 7, 13, 14\}.$$

Note that b is a code word in Shor's code and so $b \in C'$. By Theorem 1, there is an integer n and subsets A, B of Z_n such that $R \subset A$, $S \subset B$ and $Z_n = A + B$ is a factorization.

If $2 \nmid |B|$, then by Proposition 3 of [8], in the factorization $Z_n = A + B$ the factor B can be replaced by $8B$ to get the factorization $Z_n = A + 8B$. Then

$$\underbrace{0}_{\in A} + \underbrace{8}_{\in 8B} = \underbrace{8}_{\in A} + \underbrace{0}_{\in 8B}$$

contradicts the factorization. Thus $2 \mid |B|$. A similar argument gives that $3 \mid |B|$ and $11 \mid |B|$.

If $5 \nmid |B|$, then B can be replaced by $5B$ to get the factorization $Z_n = A + 5B$. Now

$$\underbrace{3}_{\in A} + \underbrace{5}_{\in 5B} = \underbrace{8}_{\in A} + \underbrace{0}_{\in 5B}$$

is a contradiction. Thus $5 \mid |B|$ and so $(2 \cdot 3 \cdot 5 \cdot 11) \mid |B|$.

Note that $\langle A \rangle = \langle B \rangle = Z_n$. By Theorem 3, $|A|$ must have at least three distinct prime divisors p_1, p_2, p_3. Hence, n is a multiple of $330 p_1 p_2 p_3$.

This completes the proof. □

References

[1] V. Bruyère, M. Latteux, Variable-length maximal codes, Lecture Notes in Comput. Sci. 1099 (1996) 24–47.
[2] C. De Felice, An application of Hajós factorization to variable length codes, Theoret. Comput. Sci. 164 (1996) 223–252.
[3] C. De Felice, On a property of factorizing codes, Internat. J. Algebra Comput. 9 (1999) 325–345.
[4] N.H. Lam, Hajós factorizations and completion of codes, Theoret. Comput. Sci. 182 (1997) 245–256.
[5] A. Restivo, S. Salemi, T. Sportelli, Completing codes, RAIRO Inform. Théor. Appl. 23 (1989) 135–147.
[6] A.D. Sands, On the factorisation of finite abelian groups II, Acta Math. Acad. Sci. Hungar. 13 (1962) 153–169.
[7] A.D. Sands, On Keller's conjecture for certain cyclic groups, Proc. Edinburgh Math. Soc. 22 (1979) 17–21.
[8] A.D. Sands, Replacement of factors by subgroups in the factorization of abelian groups, Bull. London Math. Soc. 32 (2000) 297–304.
[9] P.W. Shor, A counterexample to the triangle conjecture, J. Combin. Theory A 38 (1985) 110–112.
[10] S. Szabó, A type of factorization of finite abelian groups, Discrete Math. 54 (1985) 121–124.
[11] S. Szabó, C. Ward, Factoring abelian groups and tiling binary spaces, Pure Math. Appl. 8 (1997) 111–115.